GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Understanding VPN tunnels over SSL

Xavier Garcia Faura
February 6th, 2005

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4c, Option 1

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Table of Contents 2

Abstract 3

What is a VPN 3

What is SSL 3

What is a VPN tunnel over SSL (VPN-SSL) 4

Benefits of VPN over SSL 4

How does a VPN-SSL work 6

Possible uses and architectures 9

Risks associated with SSL VPN's 11

VPN-SSL vs. VPN-IPSec? 12

How to choose a VPN-SSL solution 12

Conclusion 15

References 16

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract

Virtual Private Networks over SSL have been around for a few years now, but they are still not widespread in the enterprises even if they bring real business value to a company's security infrastructure.
The objective of this paper is to explain these values in a simple and clear way, outlining how they can be used, what the risks are and the measures an organization can take when implementing this type of solution.

What is a VPN

The term VPN stands for Virtual Private Network, and it describes a system that allows the transport of information trough public media in a private manner. In other words, a VPN allows users or networks to privately transfer data to other systems, even when using a public transport method like the Internet.
Since Internet access began becoming more available, faster and cheaper, corporations started considering VPN tunnels over the Internet as a valid and reliable transport method for their private data, and nowadays VPNs are widely used. There are two main types of VPNs: Remote access VPNs and Site-to-site VPNs.
Remote access VPNs are normally used by roaming users who need sporadic access to their networks. These VPNs are normally established from a single machine to a remote network, and they are created and destroyed on demand, only for the time the user requires the connection.
Site-to-site VPNs are normally created to connect two remote networks, they usually give service to more than one host on each of the networks, and they are permanent connections.
VPNs can be based on three main architectures: IPSEC (IP Security), MPLS (Multiprotocol Label Switching) and SSL (Secure Sockets Layer); this paper will focus on this last technology.

What is SSL

Secure Sockets Layer (SSL) is a protocol that was originally designed by Netscape to encrypt web communications for online banking and e-commerce applications over the Internet. SSL is an official Internet standard and it is available on every web browser in common use, and in "Open Source" form. SSL was originally created to secure web traffic, but it is increasingly used to secure non-web application protocols (such as SMTP, LDAP, POP, IMAP, and TELNET). SSL provides digital certificate–based client and server authentication, integrity checking, and confidentiality. SSL provides transport-level confidentiality through secret key cryptography, and key management and authentication through public key cryptography.

© SANS Institute 2000 - 2005, Author retains full rights.

What is a VPN tunnel over SSL (VPN-SSL)

The idea behind a VPN-SSL tunnel is very simple: to use SSL instead of traditional IPSEC to encrypt the communications over the VPN tunnel that connects a remote user to the corporate network. Purists might say that this is not strictly a VPN tunnel[1] as the encryption in SSL is application centric and not communications centric, but from a user's practical point of view a VPN is an encrypted and secure channel that allows private communications through the internet to the corporation. Due to the nature of SSL the access is proxied, so the user is never directly connected to the corporate network. In addition, this access occurs at the application layer, not the network layer, which enables the administrator to control not only the internal addresses accessed, as IPSec would, but also access to the applications.
The difference between IPSec and SSL VPN tunnels might just appear as a theoretical issue, but this paper will outline how its impact on the day-to-day operation of the VPN goes much further than that.

Benefits of VPN over SSL

VPN over SSL has several benefits which make the solution very attractive when compared to traditional VPN-IPSEC tunnels:

The solution is Clientless

Traditionally VPN-IPSEC solutions require a VPN client in each of the devices to be able to connect to the network. These clients need to be installed, configured and maintained. In fact remote clients tend to be very difficult to maintain, and a big part of the cost of the VPN-IPSEC infrastructure nowadays comes from the cost of maintaining these VPN remote clients.

When using VPN-SSL this maintenance cost disappears because there is no VPN client involved in the connection. Well, there actually is a VPN-SSL client, the browser. All the SSL encryption / decryption on the client side is done by the SSL module of the browser, but this requires little or no configuration or maintenance from the IT group.

There are less interoperability issues

SSL solutions are highly interoperable. It is rare to experience problems between an SSL client and server. IPSEC, even though it is made up of a set of Internet standards, continues to suffer from interoperability problems, even among some products that conform to the standards.

There are no issues traversing firewalls

Another big problem with VPN-IPSEC clients is the presence of firewalls in the path between them and the IPSEC corporate gateway. There are two main reasons: 1) IPSEC does not traverse NATing devices well and 2) most

[1] Charlie Hosner, OpenVPN and the SSL VPN Revolution

© SANS Institute 2000 - 2005, Author retains full rights.

firewalls rule sets do not allow IPSEC traffic. Even if VPN-IPSEC manufacturers have come up with solutions to solve the NATing problem like UDP encapsulation, firewall administrators still tend to block outbound IPSEC from their networks.
When using SSL instead of IPSEC these problems disappear as SSL has no problems with NAT and firewalls normally allow SSL traffic towards the Internet, as this protocol is commonly used by web applications like on-line banking and on-line retailers.

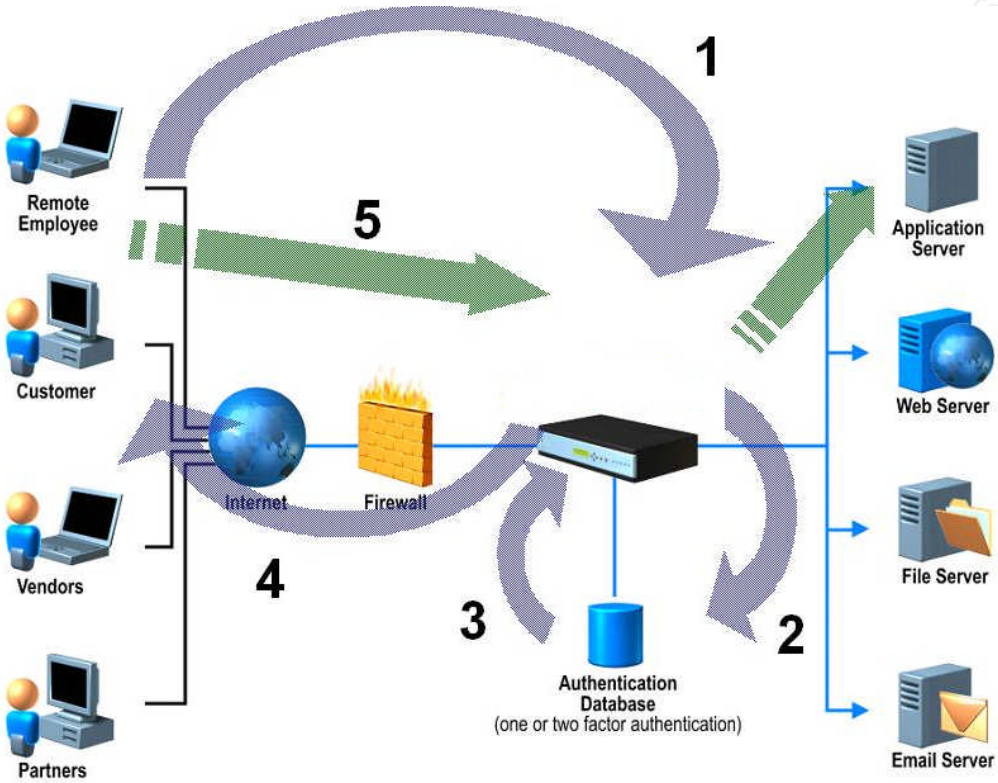
The access control is more granular

IPSec is network-layer centric while SSL is application-layer centric. That means an SSL VPN can easily ensure that users gain access only to the designated resources or applications specific to their needs, while using IPSec it is very difficult to create such precise control rules, so most organizations end up providing open access to their whole network for remote users. Basically, when you design the access rules on a SSL-VPN gateway everything is geared towards granting access to applications (layer 7), whereas in an IPSEC-VPN gateway access is normally granted to hosts or networks (layer 3).

© SANS Institute 2000 - 2005, Author retains full rights.

How does a VPN-SSL work

SSL-VPN tunnels really simplify the user experience for remote VPN's, as all the steps the user needs to follow do not require any type of technical skills. The typical connection process from a user point of view is explained below:[2]



Step 1

The user connects to the VPN-SSL web site over an https secure connection. This is an easy operation for users as they are used to accessing Internet web sites. At this point the portal prompts the user for some sort of authentication, either username and password or any type of strong authentication. In instances where the portal is facing the Internet, which is normally the case in a remote access scenario, a two-factor authentication is highly recommended as any Internet user will have access to the authentication portal and brute-force attacks, social engineering, or any other methods might be used by potential intruders to try to obtain valid credentials.

[2] Graphic from Protecting Extended Enterprise Networks with Symantec Clientless VPN Gateway

© SANS Institute 2000 - 2005 Author retains full rights.

Steps 2 & 3

The VPN gateway queries an authentication server and this returns the access authorisation to the VPN-SSL server. Most VPN-SSL solutions available in the market support a large range of authentication methods to be able to integrate swiftly in an existing corporate environment.[3]

Step 4

Once the user has been authenticated against a user database (normally an ldap server or Active Directory), the VPN gateway portal shows the user a menu with the possible applications that can be accessed by this user account. In most cases this list of applications will depend on who the user is or even on the type of authentication a user has used. Another option at this point is the automatic start-up of the application, without giving the user a list of choices. Please note here how the access is application-centric and not network centric: access to the user is granted to published applications and not to servers or network segments.

Step 5

Once the application has been selected the communication encapsulated within the SSL tunnel begins. This communication will always be proxied by the SSL-VPN gateway, which means that the client will talk to the gateway, and the gateway will relay the client queries to the application server. The communication will be established in one of the three modes described below, depending on the nature of the application.

i. Reverse Proxy

This is what will occur if the application accessed by the user is web-based. In this case the browser will send the http query to the gateway, and this will forward the same query to the web application server. In this case the SSL-VPN gateway acts just as a reverse http proxy, forwarding the user requests to the internal web application and relaying the responses back.

ii. Port Redirection

This is what happens when the user needs to access a non-web application, hence not using the client browser and standard web traffic. To better understand this take the example of a telnet session. When the user selects the telnet application on the portal an applet is downloaded to the user's PC. This applet starts capturing outgoing traffic from the PC directed to port 23 and it redirects it into the SSL tunnel. When the traffic reaches the gateway, the device just removes the SSL encapsulation and puts the original telnet traffic on the corporate network. When the user starts the telnet session all its traffic will be captured by the applet and transported to the remote network through the SSL tunnel without the user having to perform any complicated operations.

[3] See references from Symantec, Aventail, Netilla, CheckPoint and Cisco

© SANS Institute 2000 - 2005 Author retains full rights.

iii. Layer 3 encapsulation

In this situation the user will obtain full layer 3 access to the network, as in the case of a VPN IPSec connection. When the user selects this option on the portal, a virtual network adapter is downloaded and automatically installed on his device. This adapter will have an IP address on the remote network and will allow full access to it. The advantage here is that the remote machine does not need to have the VPN adapter preinstalled, as it is downloaded, installed and finally uninstalled on demand. Unfortunately, in most of the cases the user will need to have local administrative rights on its machine to be able to install and uninstall network adapters.

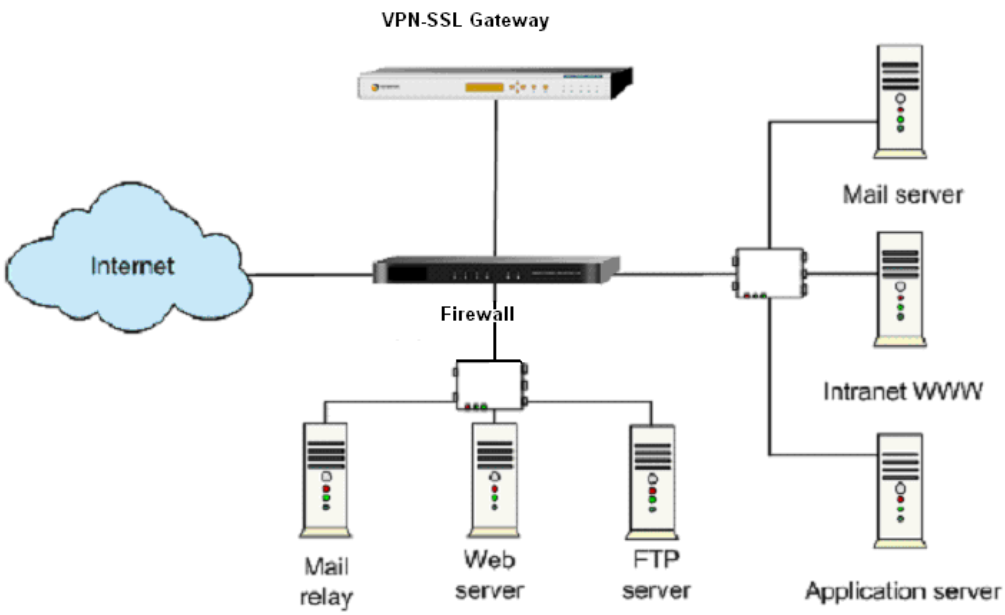
© SANS Institute 2000 - 2005, Author retains full rights.

Possible uses and architectures

The idea of this type of solution is to be able to provide access to remote users and partners without having to use a device administered and configured by the IT department. For example, an on-site consultant using a customer's PC could access his company's corporate network without having to install any software on the machine, or a company could set up a VPN-SSL gateway to allow access to outsourcing partners and limiting them on the machines and applications they could access remotely.
To provide remote access to a corporate network the VPN-SLL gateway must be accessible from the public network where the remote user is located. This leads to multiple possible architectures, but this document will focus on the three configurations that present the highest interest because they are the most common:

1. VPN-SSL gateway on a DMZ (service network)

All networks should be protected with a strong perimeter security device. This architecture has the VPN-SLL gateway as a publicly accessible corporate service protected by the perimeter security gateway. A good security design generally segregates unsecured traffic from secure traffic to prevent attacks. A benefit of placing the VPN-SSL gateway on the DMZ is that it is isolated from other publicly available servers which normally have a higher risk of being compromised. This network separation protects the gateway from attack if one of the publicly accessible servers is compromised. A potential problem with this design is that both unsecured (inbound SSL traffic) and secure (authenticated and unencrypted) traffic is carried over the same network.[4]

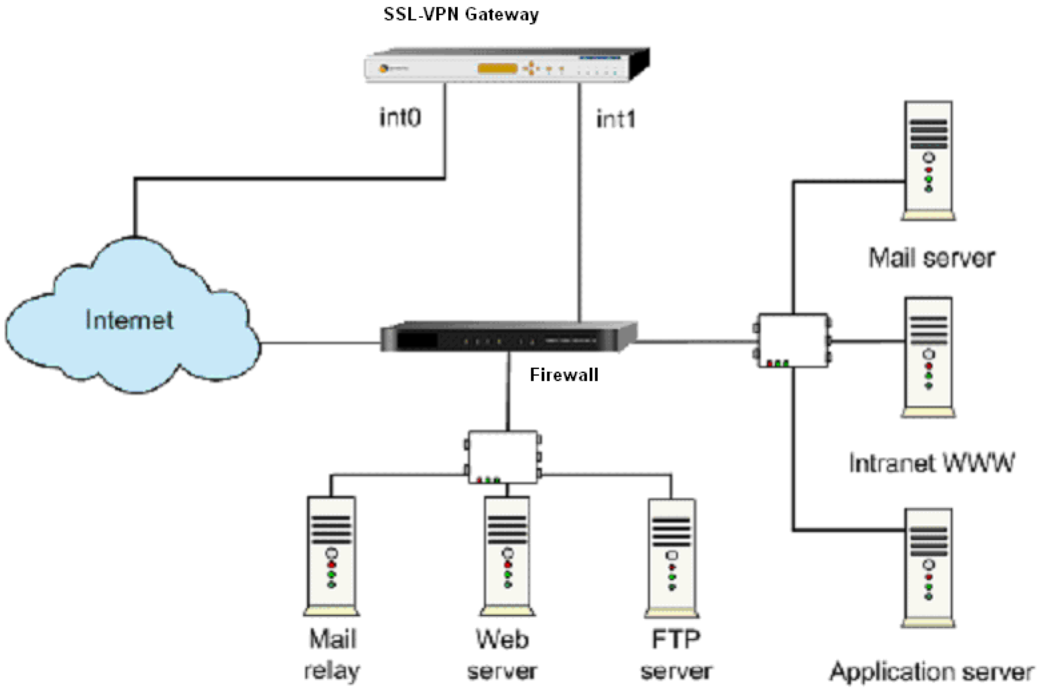


[4] Graphic courtesy of Symantec

© SANS Institute 2000 - 2005 Author retains full rights.

2. VPN-SSL gateway with 2 interfaces

In this configuration the VPN-SSL gateway is directly connected to the Internet. The second port is connected to a service network that is secured by the perimeter security gateway. The benefit of this deployment is that traffic is reduced (and resource usage) on the perimeter gateway since remote users will use the VPN Gateway first in establishing a secure tunnel to the internal network. Access control rules can be used on the SSL-VPN Gateway to further filter the traffic that is allowed to reach the perimeter security gateway providing additional security validation.[5]



A potential problem of this configuration is that the VPN Gateway is left unprotected by the perimeter security gateway. For example, the VPN Gateway could be susceptible to protocol anomaly attacks or network attacks.

3. Wireless environment

The SSL-VPN technology can also be used to secure Wireless environments. As the industry waits for a standard that will guarantee secure Wi-Fi communications, the VPN-SSL gateway can be placed between the wireless access point and the corporate network, ensuring strong encryption over the wireless media and controlling access to the corporate resources.

Risks associated with SSL VPN's

[5] Graphic courtesy of Symantec

© SANS Institute 2000 - 2005 Author retains full rights.

The idea of being able to access corporate resources from any device anywhere is obviously appealing from a business prospective, but it also brings into the security picture risks that were not present before. If the right measures are taken these risks can be minimized, and the solution will continue to bring all its advantages. The main risks could be included in the following groups:

Remote device integrity

The first point to consider in using SSL VPN's is that devices not controlled by the IT department will be connecting to the corporate network, as remote clients do not require any specific installation or pre-configuration. These remote machines might not be protected against viruses, worms, trojans, or other sources of infection, and connecting them to the corporate environment might be a risk of infection.

Some SSL-VPN gateways try to solve this problem by enforcing client integrity checks, not allowing the connection to remote devices that do not comply with a certain client security policy (antivirus, client firewall, OS patches …). This option might work in some cases but is not enough when remote users need to connect from kiosks or Internet cafés, as they have no control over the remote client.

Other SSL-VPN gateways include perimeter defense technologies like antivirus, IPS, firewall…. In this case the gateway will "clean" the client traffic at the corporate side of the VPN tunnel before it enters the network. In this situation access could, for example, be allowed to a machine infected with a worm, as the IPS will block its attacks while the user would still be able to access the published applications. This solution is easier to implement because it does not require any type of enforcement on the client side, but it might be prone to attacks on the client side, like key-loggers.

Remote device history

Other security risks come from the information stored on the browser. When a user connects to the corporate network using a browser, the web site will leave a series of traces indicating where they were and what they were doing (URL's history, cookies, applets…). If this connection was made from a public PC the information left behind might be very valuable to a possible attacker, as information like IP addresses, server names, or even cached files would be left on the browser. This is why most SSL-VPN gateways include functions that would delete most of this information when finishing the user session.

Portal accessibility

It should be considered that no pre-configured software needs to be installed on the remote device, which means that anybody with a web browser can connect to the VPN-SSL portal. This exposes remote access system to possible password attacks to obtain illegal access. This situation can be remediated by using strong authentication methods.

VPN-SSL vs. VPN-IPSec?

© SANS Institute 2000 - 2005 Author retains full rights.

It is important to note that SSL VPN's are not here to replace IPSec. Even if they bring some serious advantages to the remote user, IPSec has also its place in the VPN arena. Apart from all the SSL advantages outlined in this paper, the following points should also be considered when choosing SSL or IPSec to encrypt tunnels:

SSL VPNs are only valid for remote user access

SSL VPN's only make sense for user remote access, as they don't provide full network connectivity and they are asymmetric (client / server) solutions. For site-to-site tunnels or permanent tunnels between two machines it is still more effective to use traditional IPSec VPN.

Layer 3 access over SSL VPN is complicated

Even if some SSL-VPN solutions offer this type of feature, layer-3 access over SSL VPN is not simple, as remote users might require administration rights and, besides, this type of access goes against the SSL application-layer philosophy. In the case where this type of access is required, IPSec is still the best choice.

SSL VPN solutions are expensive

SSL VPNs are expensive compared to IPSec VPN, even if the IPSec administration costs can be much higher. In situations where the investment on the solution must be low, even if administration costs might be higher, IPSec VPN is the best choice.

How to choose a VPN-SSL solution

There are a several SSL-VPN solutions available in the market, and different products might be better suited for different scenarios. Nevertheless, there are a few technical aspects that should always be considered when choosing this type of solutions:

Gateway Architecture

It is important to understand the architecture of the SSL-VPN gateway. Most solutions are presented as VPN appliances, and in this case the solution manufacturer is normally responsible for providing patches and updates for whatever operating system and web server is installed inside the appliance. In the case of a software solution this responsibility will lay on the administrator, increasing the solution's maintenance workload. Besides, appliances normally include specialized encryption hardware to accelerate and maximize the number of possible simultaneous connections.
Some of the available solutions are global VPN tunnel endpoints, as they are able to cater for both SSL and traditional IPSec tunnels simultaneously.

Gateway Security

The SSL-VPN gateway will probably be facing the Internet, and this is why its security is extremely important. Choosing a hardened solution including DoS and SYN attacks protection would be a good choice. It is also important to

© SANS Institute 2000 - 2005, Author retains full rights.

find out which ports are opened on the outside interface, what vulnerabilities have been reported for the solution in the past, and whether they have been corrected or not.
Some SSL-VPN solutions include additional gateway security features like antivirus, IDS and IPS. It is important to consider if these functionalities will be relevant in the final environment.

Client Architecture

Most commercial solutions support Microsoft Windows clients and browsers, and in a vast majority of cases this will be enough. Nevertheless, there are solutions that support other platforms (Linux, Unix, Macintosh, PocketPC, PalmOS,…) and other browsers (Mozilla, Firefox, Netscape, …).
An important point here is to find out what type of communications (Reverse Proxy, Port Redirection and Layer 3) are supported for each operating system, what type of OS rights are necessary for the user, and whether the previous installation of a client is necessary for some of the above scenarios.

Client Security

As was mentioned before in this paper, the client is the weakest link of the SSL-VPN solutions. This is due to the fact that it is normally not controlled or administered by the IT department. A good SSL-VPN solution should be able to verify the client integrity or at least to request certain pre-requisites (antivirus, patching level, …) before the client connects. Unfortunately this type of solutions normally requires a pre-installed piece of software on the client, eliminating one of the biggest advantages of SSL-VPNs.
It is also good to check if the solution is able to remove any connection trace on the client side (URL history, cache, cookies, applets, …) when the session ends.

Authentication and Access Control

Most SSL-VPN solutions will be able to use several methods for user authentication: ldap, Active Directory, Radius, RSA, X.509 certificates, and other. It is important to check that the SSL-VPN solution can easily be integrated in a corporation's authentication infrastructure.
In some situations it might be interesting to see if the solution's access control method can be based in several factors, like user name, authentication type, client's IP address, client's OS, date & time, client integrity check, …

Applications

Even if vendors claim to support all type of applications over their VPN-SSL solution, it is important to check that the applications that will be used have been explicitly tested and verified. This is especially true when using applications like VoIP and H.323 due to the fact that they are UDP based, and this could cause additional problems on certain solutions.

Portal

The SSL-VPN portal will be the centre of the user experience, and this is why it should be fully customizable, not only with static html, but also with ActiveX

© SANS Institute 2000 - 2005 Author retains full rights.

or Java applets.
If the solution will be used within the Intranet or Extranet, it is important that the SSL-VPN portal can be integrated with the existing one.

Performance and High Availability

Performance is normally a critical factor in this type of solutions, as encryption is very resource consuming. Vendors normally scale their SSL-VPN gateways based on the number of concurrent connections supported. As this number might be sometimes difficult to calculate, the chosen solution should be scalable and provide an easy way to increase the number of users. Load balancing and failover capabilities should also be included in the solution.

Logging and Audit

It is important that the SSL-VLN solution provides extensive logging and auditing capabilities of all type of events. Integration with other logging or monitoring systems via syslog or SNMP traps would be a plus.

Administration

Administration should be performed over secure protocols like SSL or SSH, and trough a dedicated administrative network interface if possible.

Price, Product Maturity and Roadmap

Like in any other type of solutions there are non-technical factors that will come into consideration. To choose a SSL-VPN solution it will be very important to verify the product maturity and other customer references, as the technology is fairly recent. Choosing a mature solution from a well-known and stable corporation can be a good guarantee.

© SANS Institute 2000 - 2005, Author retains full rights.

Conclusion

From a theoretical point of view SSL VPN's seem to bring many advantages over traditional IPSec for remote user access. In Aventail's white paper "Comparing Secure Remote Access Options", David Thompson, Senior Research Analyst, Meta Group said "By 2005/06, SSL-based solutions will be the dominant method for remote access, with 80% of users utilizing SSL, though IPSec will still be used for specialized applications and user requirements."
But the truth is that companies have done very little to move to this technology, and most of them continue to use IPSec VPN's. On one hand SSL VPN's are not as mature as IPSec, and most corporations prefer to rely on well-known and proved technology when it comes to security. Many companies are still protecting past investments in remote access solutions however, when the time comes to replace the existing remote access systems, SSL VPN remote access systems will be the preferred choice in most remote access situations.

SSL VPN technology is still not widely understood by many IT professionals. Hopefully this paper will provide a better insight into this great technology, and little by little SSL VPN's will start to take the place they deserve in the security market.

© SANS Institute 2000 - 2005, Author retains full rights.

References

1. Symantec, Protecting Extended Enterprise Networks with Symantec Clientless VPN Gateway
https://enterprisesecurity.symantec.com/content/displaypdf.cfm?SSL=YES&PDFID=689

2. Frederick M. Avolio, Security Review: SSL VPNs
http://www.aventail.com/downloads/pdfs/Avolio_SSLVPN_SecWP.pdf

3. Aventail, SSL VPN or IPSec VPN: Which one is right for you?
http://www.aventail.com/downloads/pdfs/IPSec_vs_SSL_VPN_aventail_site.pdf

4. Aventail, The SSL VPN Technical Primer
http://www.aventail.com/documents/default.asp?OID=836&TID=836

5. Stratecast Partners, Addressing Enterprise Remote Access Challenges
http://www.f5.com/f5products/pdfs/F5_Networks_White_Paper.pdf

6. CheckPoint, SSL VPNs: The challenge of delivering both flexibility and security
http://internet.ziffdavis.com/checkpoint/images/Chkpnt_Final.pdf

7. Cisco, Enterprise Guide for Selecting an IP VPN Architecture
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns465/c654/cdccont_0900aecd801b1b0f.pdf

8. Netilla, Achieving Versatility and Network Protection in an SSL VPN
http://www.netilla.com/downloads/wp_achieving_versatility_protection.pdf

9. Netilla, A Comparison of VPN Solutions: SSL vs. IPSec
http://www.netilla.com/downloads/wp_ipsec-vs-ssl.pdf

10. Charlie Hosner, OpenVPN and the SSL VPN Revolution
http://www.sans.org/rr/whitepapers/vpns/1459.php

11. Steven Ferrigni, SSL Remote Access VPNs. Is this the end of IPSec?
http://www.sans.org/rr/whitepapers/vpns/1285.php

12. Javier Zubieta, Accesos remotos seguros a través de SSL-VPNs
Revista SIC, nº 58, págs. 75-75, Febrero 2004

© SANS Institute 2000 - 2005 Author retains full rights.